Alkadhum Journal of Science, Vol. 1, No. 2 (2023)

Open Access ISSN: 3005-2386 (Online), ISSN: 3005-2378 (Print)

IRAQI Academic Scientific Journals

Alkadhum Journal of Science (AKJS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

AKJS Alkadhum Journal of Science

Enhancement the Security by creating ontology-based Trust Management using Semantic Web tools

[1,2]Wurood Al-shadood*

[1]Education Directorate of Thi-Qar, Ministry of Education, Iraq

[2] Department of Computer Techniques Engineering, Imam Al-Kadhum College, Iraq

Article information

Article history:
Received: November, 10, 2023
Accepted: December, 10, 2023
Available online: December, 14, 2023

Keywords:
Trust Management (TM),
Ontology; Semantic Web (SW),
Web Ontology language (OWL)

Corresponding Author:
Wurood Al-shadood
worod.murad@alkadhum-col.edu.iq

DOI:
https://doi.org/10.61710/akjs.v1i2.58

Abstract

The most traditional policy models which do not consider dynamic nature of distribute systems and the limitation in addressing issues like adaptability, extensibility, and reasoning over security policies. The main cause of the flexibility and scalability issues in the environments of the Internet and dynamic networks is that there is no central control over the environments, and users are not predetermined. As a result, security and trust issues become critical in the various systems; enhancing the security of these environments would require adding trust to the existing security infrastructures. Few trust models have taken into account the semantic relationship for pervasive elements, despite the fact that numerous models have been proposed to address trust issues in dynamic environments; especially those who related to trust categories. In our work, we solve issues resulted from security and tracking the dynamics of participating communication devices in dynamic distributed networks. Through using ontology for trust management which it is define vocabularies used to described and represented an area of knowledge. For representation, we used semantic web's tools to represent the domain of the dynamic environment and we improv that the reasoning succusses in inference the trusted device and user exactly where we do query.

1. Introduction

In field of network computer, the distribution network means that a software task accomplished by dividing it into sub -tasks and each node will take care of that task. On other hand, the dynamic nodes are entering or leaving the domain of that network, the places and times of these devices will change due time. Usually, the nodes of these networks been heterogeneity.

In order to capture the heterogeneity, dynamicity can use the ontology. On the Semantic Web, ontology is seen as the answer to data heterogeneity, and matching ontologies is a highly effective way to solve the issue [1]. Ontologies are logical theories that represent the important role of semantic domains [2]. This mean can represent field knowledge by its, our ontology represents the trust management (TM) which identified as a method of establishing a relationship of trust between entities [1]. In dynamic distributed [3] systems the trust is a very important. Although, the Protege environment used as a tool during the design stage.

1.1. The Ontology Concepts

In philosophy, ontology is the essential branch of metaphysics, but in a computer science and information science, an ontology formally defines (a common set of terms that are used to describe and represent a domain). An ontology according as define in resources like in [4]: An ontology defines the terms used to describe and represent an area of knowledge; ontologies are logical theories that represent the important role of semantic domains.

Also, the encoded knowledge will include a collection of rules and can be the human experts captured to address a complex problem [5]. It is describing a basic terminology for researchers requiring information sharing in a domain.

It is from the necessary to develop an ontology. And there are some reasons for that [6]:

- To share a common knowledge of the information structure between persons or application Providers.
- To allow domain knowledge to be used again.
- To explicitly state domain assumptions.
- To stay domain knowledge, separate from operational knowledge.
- Domain Knowledge Analysis.

In general, the ontology includes (classes (concepts), object property, data property, individual instances) [6,7].

1.2. The Semantic Web (SW)

software promotes data sharing and reuses [8]. Through its technology, it makes it easier for different distributed actors on the web to share, use, and transmit knowledge and information [9]. Semantic Web depends on technologies as follows:

- Uniform Resource Identifier (URI)
- Resource Description Framework Schema (RDFS)
- Resource Description Framework (RDF)
- Web Ontology Language (OWL)
- SPARQL (Sparql Protocol and RDF Query Language)
- Semantic Web Rule Language (SWRL)
- DL- Reasoning (Description Logic- reasoning)
- XML: Extensible Markup Language

1.3. Problem statement

The main problem lies in the fact that some researchers consider that security can only be solved in authorization by giving the authorized person, for example, his own email and password, but this is not sufficient to protect the systems, so managing trust in the trusted person and his tool that logs into the system adds another security ring, and the system will become more secure. Although there is another problem related with this domain:

1. Difficult maintaining and tracking the dynamics of participating communication devices.

2. Difficulty knowing the manufacturing characteristics of entities entering contacts.

1.4. The suggest solution

We provide the solution for these problems, by using ontology representation (OWL (Web ontology language) to represent the domain of the dynamic environment. The ontology functions as a tool to capture the variety of the represented entities, which means it offers security for the system and gives semantic information for the devices through its representation.

2. Related Work

Kravari et al. [9] introduced definition and integration in general ontology of social and non-social criteria involved in IoT that will help trust management. but in their work, they didn’t employ user identity for recognition and management and didn't use Semantic Web metadata. In Kammnet et al. [10] SDN (software defined network) architecture, which is based on trust management and access control for IoT, is provided to enhance the protection of past work. But what's going to happen as the characteristics are many? this triggers the in-network complexity and prevents it from functioning. Their methodology aims to improve resource protection through the use of Trust management clustering techniques. However, a network with too many attributions will become less efficient, and devices with less processing power will become slower. It is known that reputation is derived from the past behavior of the entity/ node. Mousa et al. [11] suggested a trust architecture based on the Dependency Network for the administration of context-aware web services. Espositoa et al. [12], offer a method for handling diversity in complex distributed networks. by using fuzzy logic in conjunction with sufficient tools to handle heterogeneous fuzzy sets. They put forth a method for combining the quantitative and qualitative aspects of trust score specifications in order to calculate new degree of trust on a regular basis while taking reputational scores gathered from various infrastructure systems into account. At Amaral et al. [13], the authors introduced Unified Foundational Ontology (UFO) phase. they suggest something concrete, precisely the Reference Ontology of Trust, which they use to suit the various viewpoints contained in the literature. Within their study, they differentiate between two forms of trust (i.e. social trust) and institutional trust. In addition, they referred to the relationship between risk and trust and to the way the risk of trust relationships arises. In this sense, it is important to examine the notions of terror, economic preference, value, economic transactions, contracts, goals, social roles and control. They reflect their ontology in OntoUML, regardless of how time is spent in this respect, or whatever law is applied.

3. Methodology

The essential idea of the composition TMO split into special characteristics of   the trusted device (s) of the users and special characteristics for the user of the device (s) to facilitate the management of a trust, also to ensure firstly from the user (Done) and secondly, from his device is trusted especially in the case of a student. There are eleven primary classes in the 〖TM〗_O ontology of our framework: Can View, User, Device, Certificate , Division, Email, Done, Features, UnDone, Trusted, and Untrusted. 〖TM _O. It consists of a number of crucial objects and data properties that connect the various components of the system environment. Also, during the design and implementation stages, individuals that mirror the concepts (classes) of the 〖TM_O are added. To ensure that the ontology of the model is developing appropriately and to verify the ontology engineering process, a small number of individuals are included throughout the design phase. The huge individual sizes are added at runtime in order to verify the suggested model's dynamic behavior. The 〖TM_O ontology's primary classes are depicted in Figure (1). The class Trusted and its subclasses 〖Trusted〗_i, 1≤i≤n, for some positive integer n, are the mainstays of the 〖TM〗_O ontology. Every class 〖Trusted〗_i has an OWL complex class definition that outlines the qualities that every trusted entity needs to possess. For instance, Trusted2 is defined to indicate that an entity is considered trustworthy if it possesses the attributes listed in Formula 1.

Trusted2 = Device and (belongs_To some (User and (is_Employee some Employee) and (has_Password value "Password6")and (has_UserID value "RBGG567")and (responsible_For value "issuing_Certificates"))) and (has_MAC_Address value "GG-80-YY-17-D9-A1")

Formula 1. Trusted2 class definition

Every class within the OWL ontology is a direct or indirect subclass of the class Thing, it is important to remember this.

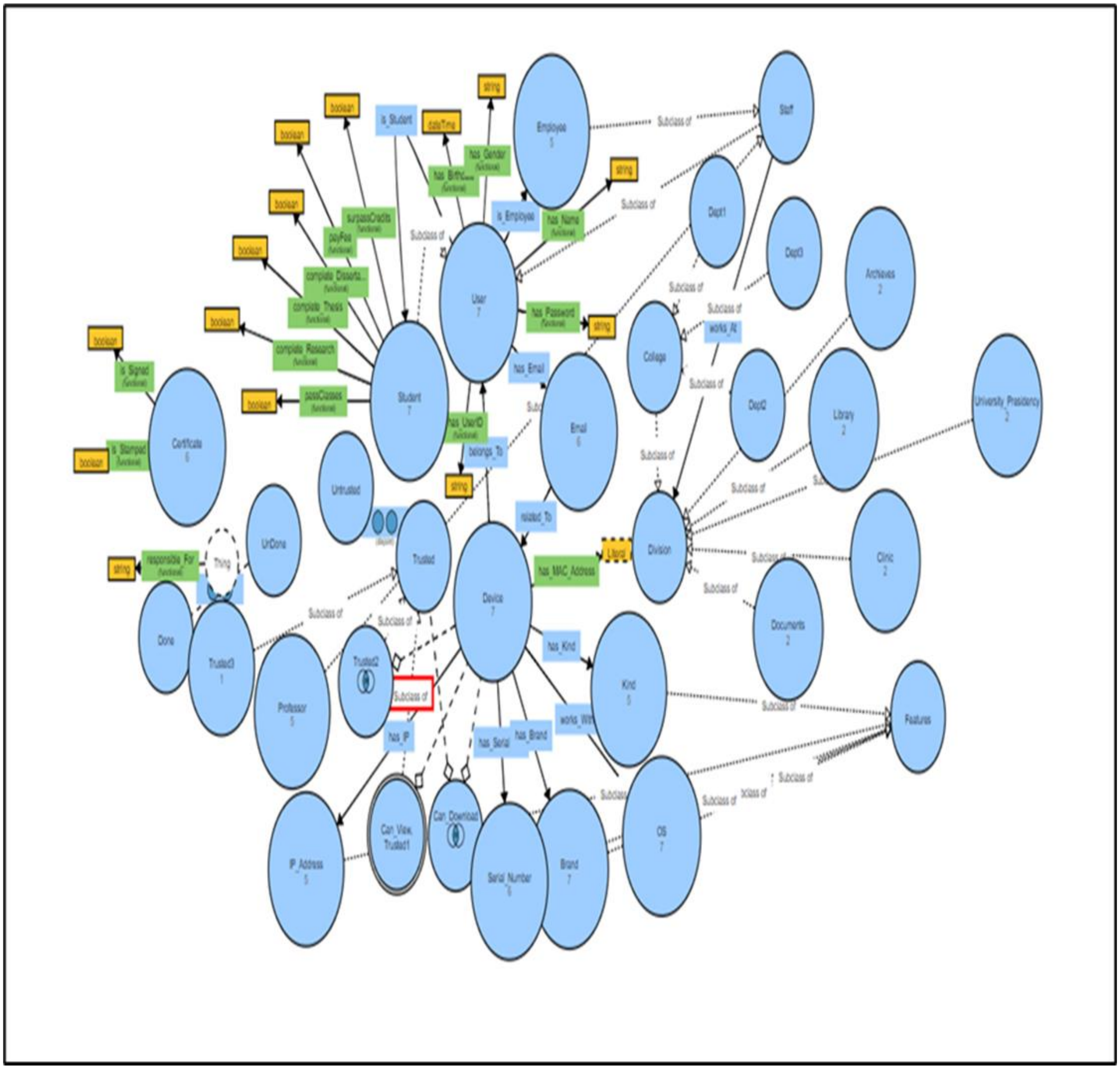
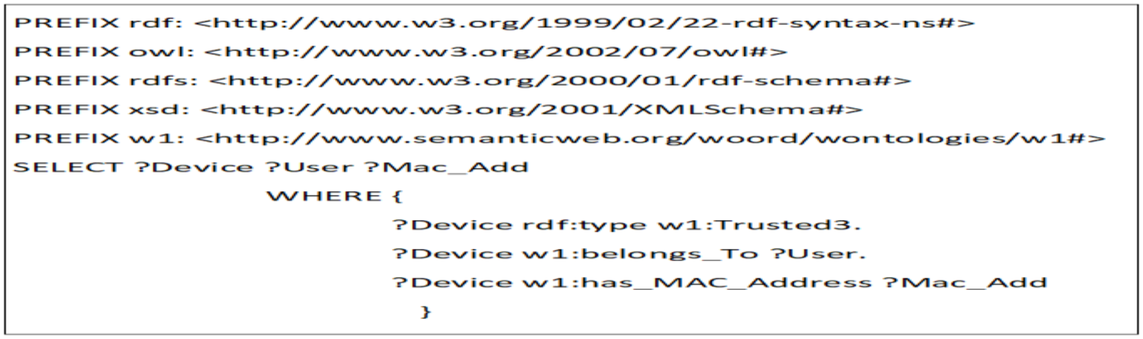


Figure (1): visual ontology, data properties (yellow), object properties (green), classes (blue).

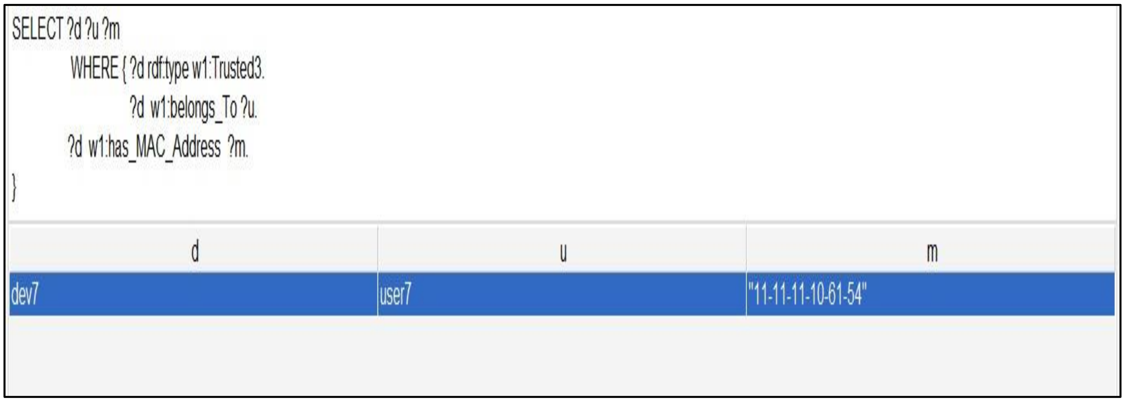
4. Implementation

The implementation includes designing the ontologies by protégé tool kit, We improve that the reasoning success in inference the trusted device exactly where we do query as shown in Figure (2), and the results of the query is shown in Figure (3).



```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX w1: <http://www.semanticweb.org/woord/wontologies/w1#>
SELECT ?Device ?User ?Mac_Add
                    WHERE {
                             ?Device rdf:type w1:Trusted3.
                             ?Device w1:belongs_To ?User.
                             ?Device w1:has_MAC_Address ?Mac_Add
                               }
```

Figure (2): A knowledge base SPARQL query



```
SELECT ?d ?u ?m
     WHERE { ?d rdf:type w1:Trusted3.
          ?d w1:belongs_To ?u.
     ?d w1:has_MAC_Address ?m.
}
```

d	u	m
dev7	user7	"11-11-11-10-61-54"

Figure (3): The Results of the SPARQL query TMO ontology

5. Conclusions and future work

could offer further security within Dynamic Distributed Networks (DDNs), for example, by making system resources resistant to various types of untrusted attempts to access them. Our approach separates between trust of device of user and the user himself by ensure from the trusted device in first then allow to the user login of same device, this work contributed in solve the community issues such that system of certificates student with which provide force security framework and protect the resources. An ontology (OWL and Rdf) capture heterogeneity, and dynamicity, in future we will use the deep learning or Machin learning to represent another secure line .

References

[1] Xue, Xingsi, and Qihan Huang. "Generative adversarial learning for optimizing ontology alignment." Expert Systems 40.4 (2023): e12936..

[2] Eriksson, Owen, and Pär J. Ågerfalk. "Speaking things into existence: Ontological foundations of identity representation and management." *Information Systems Journal* 32.1 (2022): 33-60.

[3] Wermund, Rahul. Privacy-Aware and Reliable Complex Event Processing on the Internet of Things-Trust-Based and Flexible Execution of Event Processing Operators in Dynamic Distributed Environments. Diss. Technische Universität, 2018.

[4] Li, Huaizhi, and Mukesh Singhal. "Trust management in distributed systems." *Computer* 40.2 (2007): 45-53.

[5] Gawich, Mariam. "Knowledge Representation: A Comparative Study." *Internet of Things—Applications and Future*. Springer, Singapore, 2020. 365-375.

[6] Karthik, N., and V. S. Ananthanarayana. "An ontology-based trust framework for sensor-driven pervasive environment." *2017 Asia Modelling Symposium (AMS)*. IEEE, 2017.

[7] Noy, Natalya F., and Deborah L. McGuinness. "Ontology development 101: A guide to creating your first ontology." (2001).

[8] Zeng, Marcia Lei, and Philipp Mayr. "Knowledge Organization Systems (KOS) in the Semantic Web: a multi-dimensional review. "International Journal on Digital Libraries 20.3 (2019): 209-230.

[9] Kravari, Kalliopi, and Nick Bassiliades. "Ordain: An ontology for trust management in the internet of things." OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer, Cham, 2017.

[10] Kammoun, Nadia, et al. "A New SDN Architecture Based on Trust Management and Access Control for IoT." *Workshops of the International Conference on Advanced Information Networking and Applications*. Springer, Cham, 2020

[11]Mousa , Afaf, Jamal Bentahar, and Omar Alam. “Dependency Network-based Trust Management for Context-Aware Web Services.” *Procedia Computer Science* 151 (2019): 583-590.

[12] Esposito, Christian, et al. "Trust management for distributed heterogeneous systems by using linguistic term sets and hierarchies, aggregation operators and mechanism design." *Future Generation Computer Systems* 74 (2017): 325-336.

[13] Karuna, Prakruthi, Hemant Purohit, and Vivian Motti. ": User's Trust Profile Ontology-Modeling trust towards Online Health Information Sources." *arXiv preprint arXiv:1901.01276* (2019).

[14] Bellavista, Paolo, and A. Montanari. "Context awareness for adaptive access control management in IoT environments." Secur. Priv. Cyber-Phys. Syst.: Found. Princ. Appl 2.5 (2017): 157-178